Cloud Security Processes & Practices

Jinesh Varia

Overview

- Certifications
- Physical Security
- Backups
- EC2 Security
- S3 Security
- SimpleDB Security
- SQS Security
- Best Practices

amazon web services™

AWS Security White Paper

- Available on http://aws.amazon.com
- Second version now being drafted.
- Feedback appreciated.

amazon web services™

Amazon Web Services:
Overview of Security Processes

September 2008
(Please consult http://aws.amazon.com/ for the latest version of this paper)

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data center not facing the Internet. Ensuring the confidentiality, integrity, and availability of customer's systems and data is of the utmost importance to AWS, as is maintaining trust and confidence. This document is intended to answer customer questions such as "How does AWS help me ensure my data is secure?" Specifically, AWS physical and operational security processes are described for network and infrastructure under AWS' management, as well as service-specific security implementations.

amazon web services™

AWS Certifications

- Working to ensure continued Sarbanes-Oxley (SOX) compliance.
- Working toward SAS70 Type II certification.

- Goal: validate efficacy and efficiency of internal controls.
- We'll be pursuing additional certifications.
- Developers are building HIPAA-compliant healthcare applications now.

amazon web services™

Physical Security

- We've been building large-scale data centers for many years.
- Important attributes and features:
  - Non-descript facilities
  - Military-grade perimeter control berms
  - Strictly controlled physical access (perimeter and building)
  - 3 or more levels of two-factor authentication
- Controlled, need-based access for Amazon and AWS employees.
- All physical and electronic access is logged.

amazon web services™

Data Backups

- Data stored in Amazon S3, Amazon SimpleDB, and Amazon EBS is stored **redundantly** in multiple physical locations.
- Amazon S3 replicates customer objects across multiple storage systems in multiple datacenters to ensure durability. This durability is equivalent to more traditional backup solutions, but offers much higher data availability and throughput.
- Data stored in Amazon EC2 must be proactively copied to Amazon EBS and/or Amazon S3 for redundancy

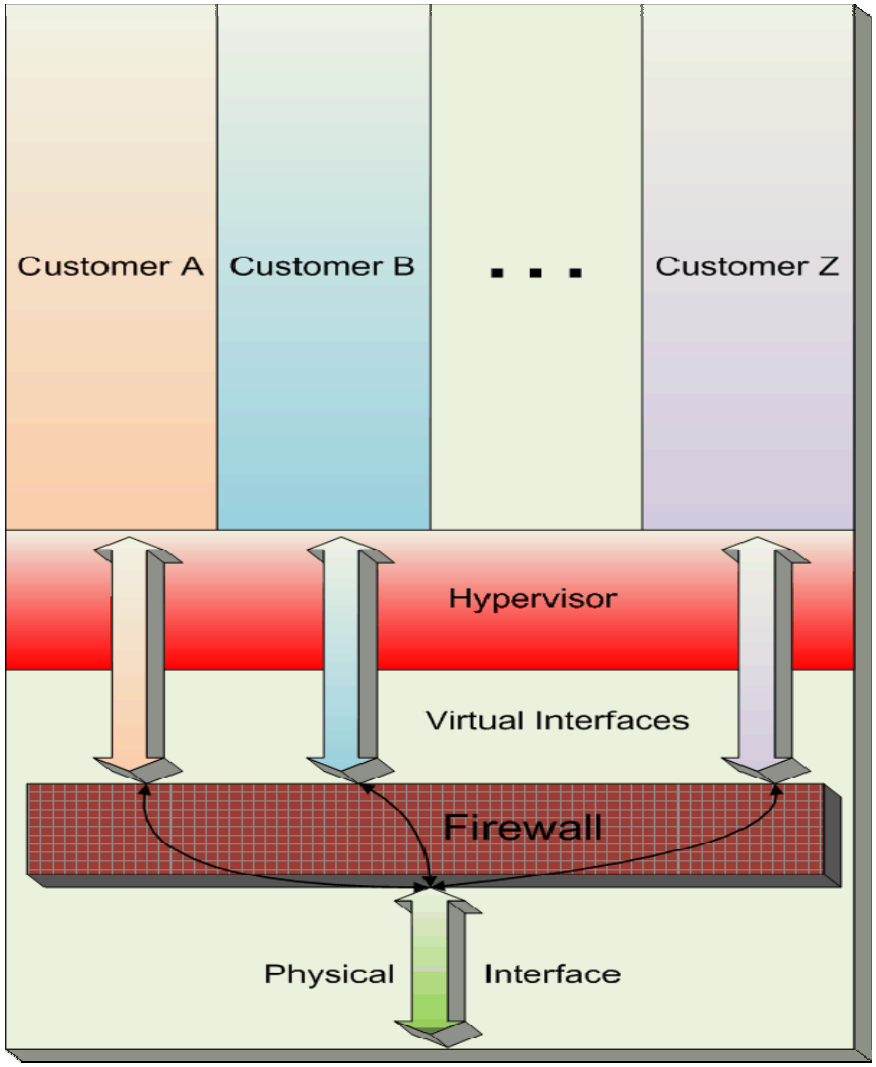
Multiple Levels of EC2 Security

- Host operating system
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- Guest operating system
  - Customer controlled at root level
  - AWS admins cannot log in
  - Customer-generated keypairs
- Stateful firewall
  - Mandatory inbound firewall, default deny mode
- Signed API calls
  - Require X.509 certificate or customer's secret AWS key

EC2 Virtualization

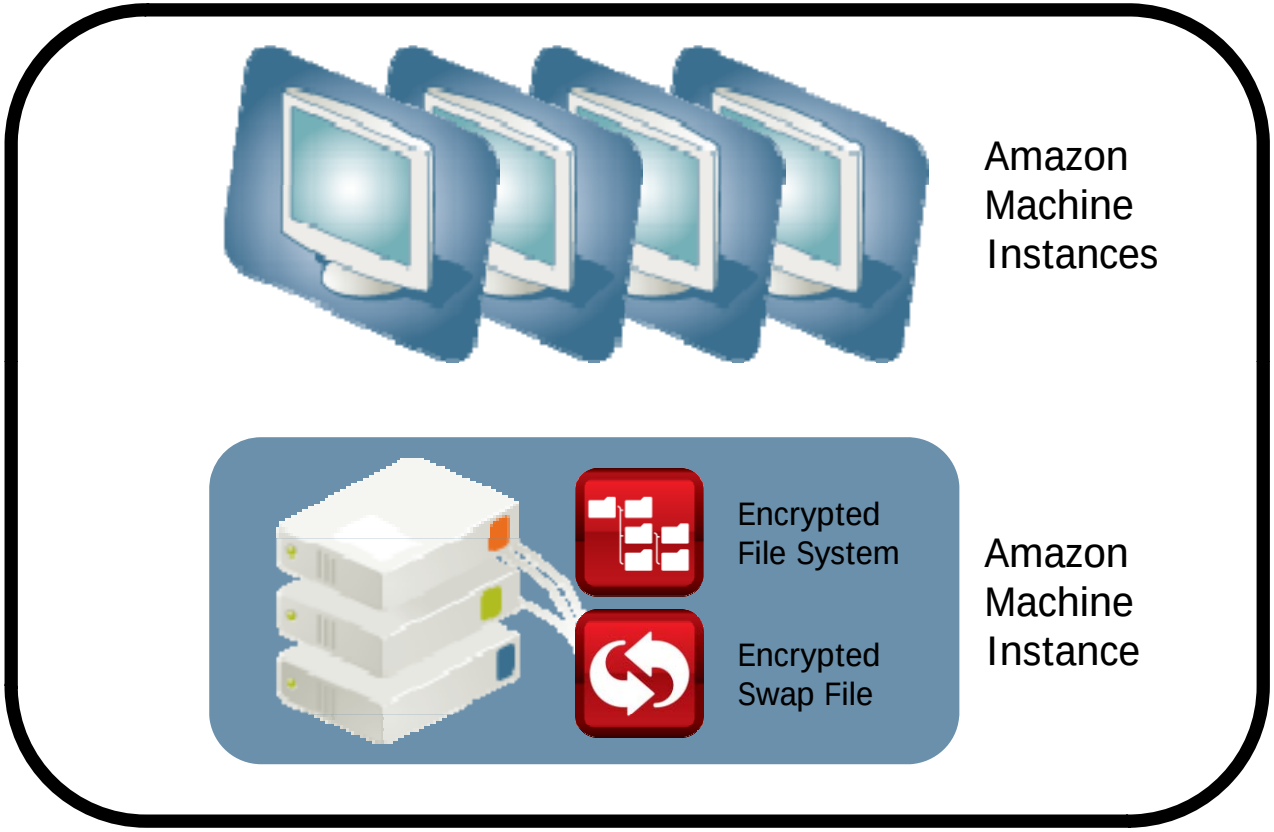
- EC2 Hypervisor:
  - Guest operating system doesn't have elevated privilege level.
  - Instances are completely isolated.
  - Intrinsic network firewall.
  - No access to raw devices.
  - Virtualized disks, logically isolated, wiped clean after use.

EC2 Instance Isolation



amazon web services™

Virtual Memory and Local Disk



- Proprietary Amazon disk management prevents one AMI from reading the disk contents of another AMI
- Local disk storage can also be encrypted by the customer for an added layer of security

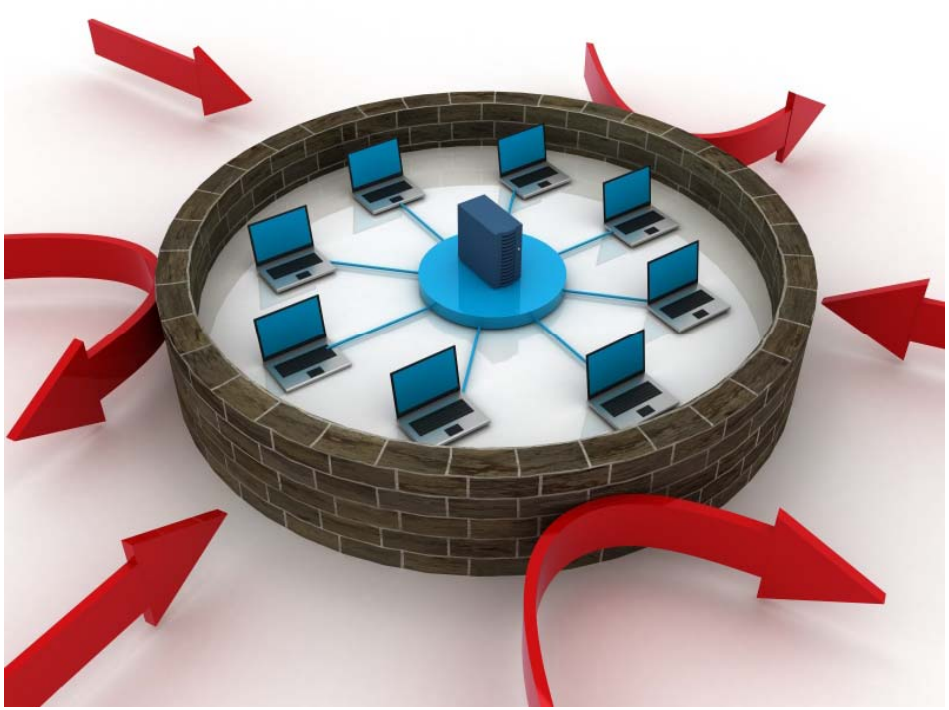
amazon web services™

EC2 Security Recommendations

- Host-based firewall (e.g. iptables) for inbound and outbound traffic.
- SSL encryption of API calls while in transit.
- Data encryption – encrypted swap and filesystem. Resources:
  - Wikipedia list of cryptographic file systems
  - Linux HOWTO

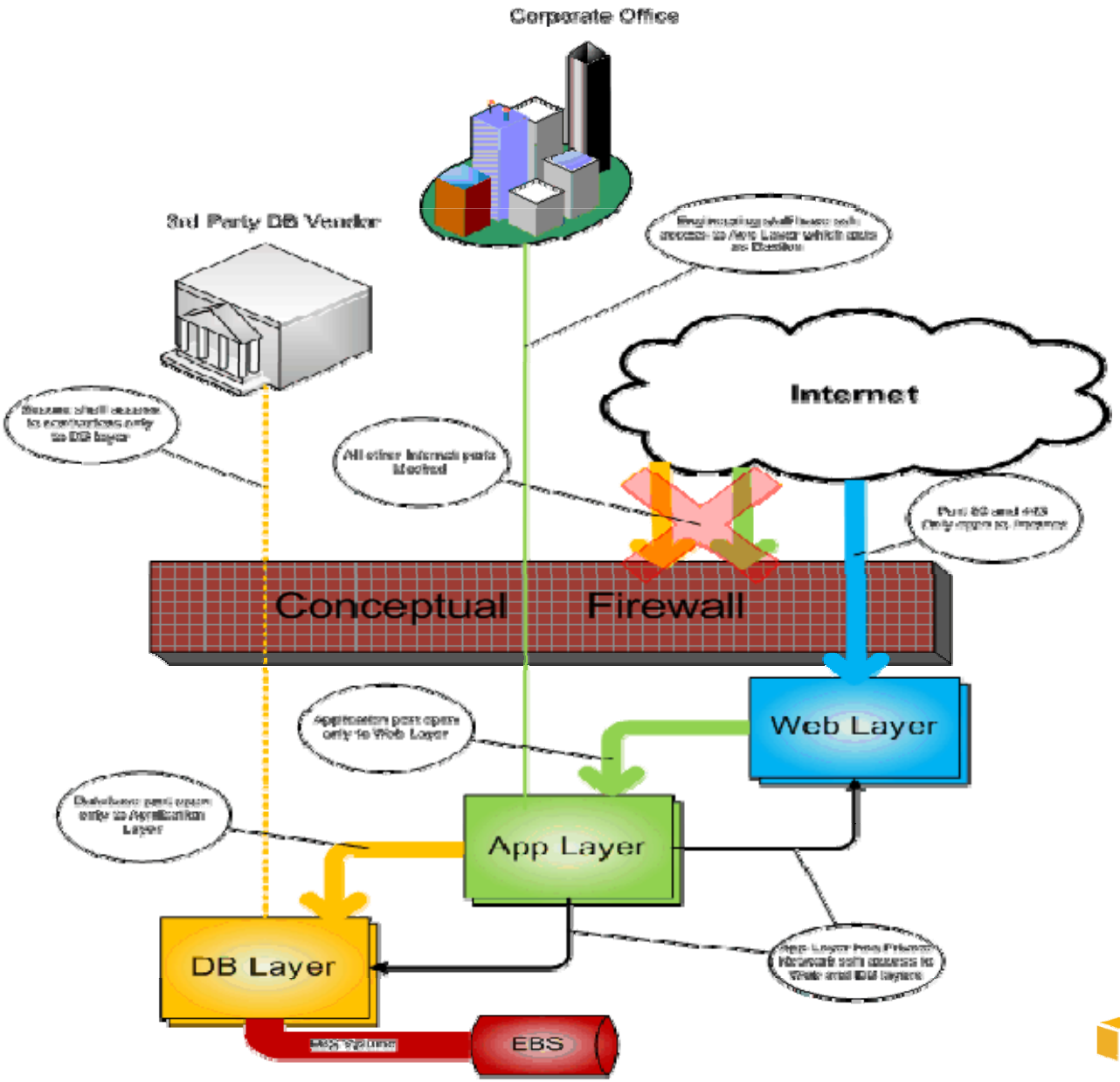
Network Security Considerations

- DDoS (Distributed Denial of Service):
  - Standard mitigation techniques in effect.
- MITM (Man in the Middle):
  - All endpoints protected by SSL.
  - Fresh EC2 host keys generated at boot time.
- IP Spoofing:
  - Prohibited at host OS level.
- Port Scanning:
  - Violation of AWS TOS.
  - Detected, stopped, and blocked.
  - Ineffective anyway since inbound ports blocked by default.
- Packet Sniffing:
  - Promiscuous mode is ineffective.
  - Protection at hypervisor level.



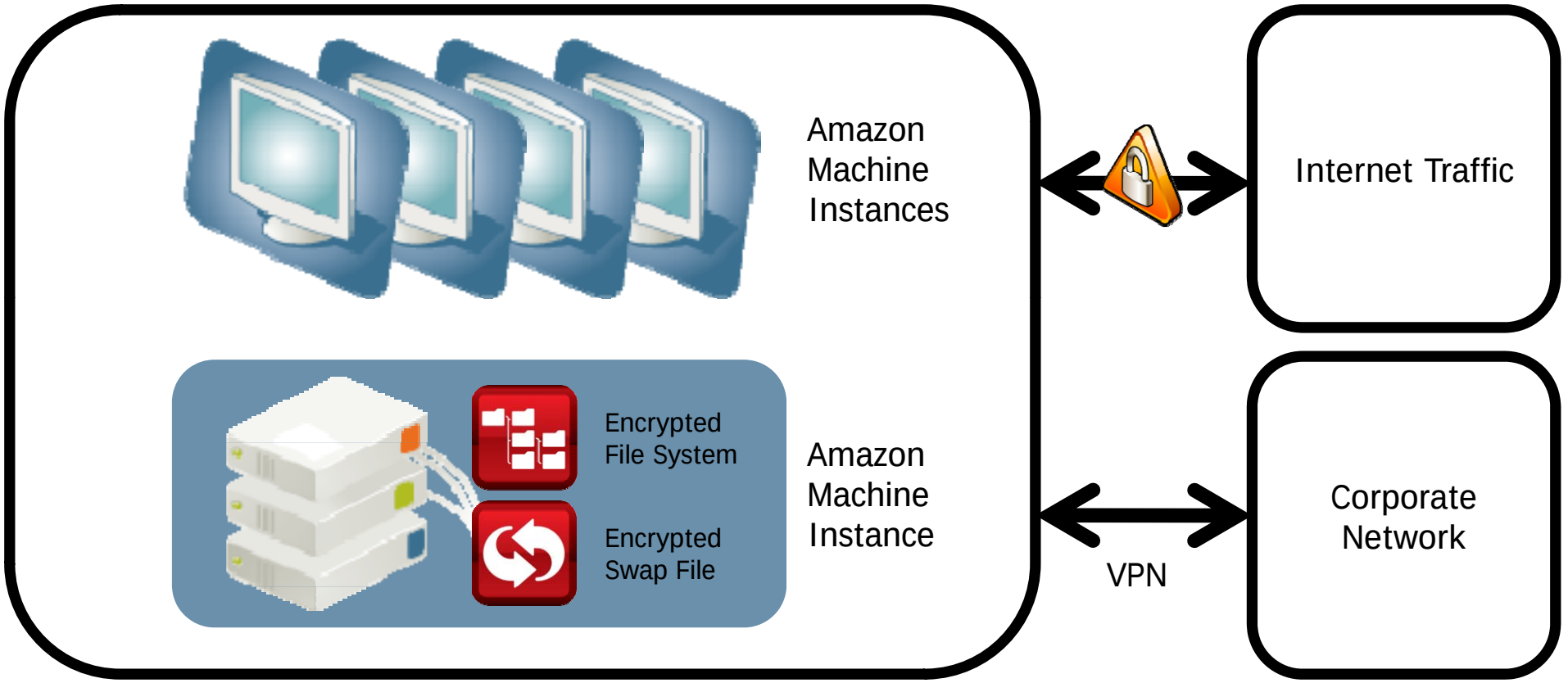
amazon web services™

Multi-tier Security Architecture



amazon web services™

Network Traffic Confidentiality

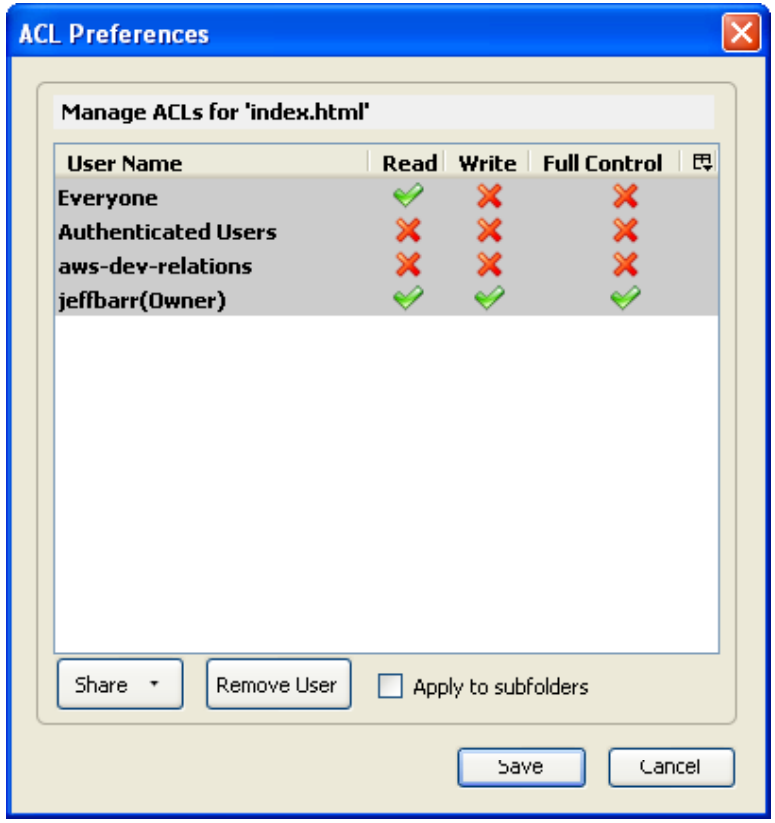


- All traffic should be cryptographically controlled
- Inbound and outbound traffic to corporate networks should be wrapped within industry standard VPN tunnels

amazon web services™

Amazon S3 Security

- Access controls at bucket and object level:
  - Read
  - Write
  - Full
- Owner has full control.
- SSL to protect data in transit.
- Encrypt when stored.



amazon web services™

Amazon SimpleDB Security

- Access based on AWS account.
- Domains accessible only to owner.
- SSL to protect data in transit.
- Encrypt data elements not used as keys.

Questions?